UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/092,401	03/05/2002	Kelan C. Silvester	42390P13005	7956

8791 7590 07/12/2005

BLAKELY SOKOLOFF TAYLOR & ZAFMAN
12400 WILSHIRE BOULEVARD
SEVENTH FLOOR
LOS ANGELES, CA 90025-1030

EXAMINER	
CERVETTI, DAVID GARCIA	

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 07/12/2005

Please find below and/or attached an Office communication concerning this application or proceeding.

Office Action Summary	Application No.	Applicant(s)	
	10/092,401	SILVESTER, KELAN	
	Examiner	Art Unit	
	David G. Cervetti	2136	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE 3 MONTH(S) FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *05 March 2002*.

2a)☐ This action is **FINAL**. 2b)☒ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-36* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-36* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☒ The specification is objected to by the Examiner.

10)☒ The drawing(s) filed on *05 March 2002* is/are: a)☐ accepted or b)☒ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

Drawings

1. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they do not include the following reference sign(s) mentioned in the description: 310 (page 9, paragraph 46, line 4, perhaps 210 was intended), 404 (page 13, paragraph 54, line 11, perhaps 402 was intended), 360 (page 14, paragraph 59), 220, 362 (page 15, paragraph 59). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

2. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference character "250" has been used to designate both "device authentication database" and "network interconnectivity" (figure 2A). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of

an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

3. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(5) because they include the following reference character(s) not mentioned in the description: 210 (figure 2A), 340, 330, 320, 322, 404, 410, 480, 490 (figure 4), 402, 562 (figure 5), 610, 670, 680 (figure 6), 710 (figure 9), 754 (figure 12), 802, 810 (figure 16), 842, 844 (figure 19). Corrected drawing sheets in compliance with 37 CFR 1.121(d), or amendment to the specification to add the reference character(s) in the description in compliance with 37 CFR 1.121(b) are required in reply to the Office action to avoid abandonment of the application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

4. The drawings are objected to as failing to comply with 37 CFR 1.84(p)(4) because reference characters "360" and "402" have both been used to designate "CPU Core" (page 13, paragraph 54). Corrected drawing sheets in compliance with 37 CFR 1.121(d) are required in reply to the Office action to avoid abandonment of the

application. Any amended replacement drawing sheet should include all of the figures appearing on the immediate prior version of the sheet, even if only one figure is being amended. Each drawing sheet submitted after the filing date of an application must be labeled in the top margin as either "Replacement Sheet" or "New Sheet" pursuant to 37 CFR 1.121(d). If the changes are not accepted by the examiner, the applicant will be notified and informed of any required corrective action in the next Office action. The objection to the drawings will not be held in abeyance.

Specification

5. The disclosure is objected to because of the following informalities: "process clock 828" (page 22, paragraph 87, perhaps "block" was intended). Appropriate correction is required.

Claim Rejections - 35 USC § 103

6. The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are such that the subject matter as a whole would have been obvious at the time the invention was made to a person having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the manner in which the invention was made.

7. Claims 1-20 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakakita et al. (US Patent Number: 6,782,260) and Cook et al. (US Patent Number: 6,718,172), and further in view of Rowland et al. (US Publication Number: 2002/0129264).

Regarding claims 1 and 11, Nakakita et al. teach detecting a wireless device within communication range of a host device (Nakakita's scheme is related to the Bluetooth protocol which provides an automatic discovery process or sensing technology); authenticating the detected device according to requested device identification information of the detected wireless device (column 7, lines 45-67, column 8, lines 1-67). Nakakita et al. do not disclose expressly when the detected device fails authentication, requesting audio authentication initialization information from the detected device; and authenticating the detected device based on the requested audio authentication initialization information. However, Cook et al. teach the use of wireless voice authentication and transaction validation, a microphone to receive a speech sample from the device user, and transferring the speech sample from the wireless device to the wireless interface (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the

invention was made to authenticate a device based on received audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art. The combination of Nakakita et al. and Cook et al. do not expressly teach switching to a different authentication method. However, Rowland et al. teach switching to different authentication methods (page 5, paragraph 76-78). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to switch authentication methods after a first authentication method used does not authenticate a device. One of ordinary skill in the art would have been motivated to do so to provide an alternative authentication method on the event of a security compromise (Rowland et al., page 5, paragraph 76).

Regarding claims 2 and 12, the combination of Nakakita et al., Cook et al., and Rowland et al. teaches the limitations as set forth under claims 1 and 11 respectively above. Furthermore, Cook et al. teach receiving an audio device authentication set-up request from a user of a wireless device (column 7, lines 50-67); requesting audio device identification information for the detected device (column 7, lines 50-67); and storing the received audio device identification information as an authentication initialization token for the detected wireless device (column 7, lines 50-67).

Regarding claims 3 and 13, the combination of Nakakita et al., Cook et al., and Rowland et al. teaches the limitations as set forth under claims 2 and 12 respectively above. Furthermore, Cook et al. teach storing the authentication initialization token within the detected wireless device (column 7, lines 50-67).

Regarding claims 4 and 14, the combination of Nakakita et al., Cook et al., and Rowland et al. does not expressly disclose compressing the received audio device identification information; and generating a hash value of the compressed audio device identification information to form the authentication initialization token of the wireless device. However, Examiner takes Official Notice that the use of compression of identification information and generating hash values of identification information was well known in the art at the time the invention was made. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compress the received audio device identification information; and to generate a hash value of the compressed audio device identification information to form the authentication initialization token of the wireless device since Examiner takes Official Notice that it was conventional and well known.

Regarding claims 5 and 15, the combination of Nakakita et al., Cook et al., and Rowland et al. does not expressly disclose polling a surrounding area of the host device for audio sources within a predetermined distance of the host device; and when an audio source is detected, initiating an authentication handshake with an audio source device of the detected audio source. However, Nakakita et al. teach polling (Bluetooth protocol which provides an automatic discovery process or sensing technology) and authenticating a wireless device (column 7, lines 45-67, column 8, lines 1-67). Furthermore, Cook et al. teach the use of audio/voice authentication with wireless devices (column 7, lines 50-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to poll a surrounding area of

the host device for audio sources within a predetermined distance of the host device; and when an audio source is detected, initiate an authentication handshake with an audio source device of the detected audio source. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication and the use of polling an area by host devices was well known in the art.

Regarding claims 6 and 16, the combination of Nakakita et al., Cook et al., and Rowland et al. teach the limitations as set forth under claims 1 and 11 respectively above. Furthermore, Nakakita et al. teach requesting the device identification information from the detected wireless device (column 7, lines 45-67, column 8, lines 1-67, column 9, lines 1-67); comparing the requested device identification information with stored device authentication information within the host device (column 10, lines 1-67). Furthermore, Cook et al. teach the use of audio/voice authentication with wireless devices (column 7, lines 50-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to establish an audio link with the detected wireless device when matching device identification information is found; and otherwise, initiating a request for audio authentication initialization information of the detected wireless device.

Regarding claims 7 and 17, the combination of Nakakita et al., Cook et al., and Rowland et al. teach the limitations as set forth under claims 1 and 11 respectively above. Furthermore, Nakakita et al. teach receiving device identification information as the requested authentication/ identification information (column 7, lines 45-67, column 8,

lines 1-67, column 9, lines 1-67); comparing the requested device authentication initialization token to one or more stored device authentication tokens (column 10, lines 1-67); and when a matching stored authentication token is detected, storing the requested device identification information of the detected wireless device as a device authentication token (column 10, lines 1-67). The combination of Nakakita et al., Cook et al., and Rowland et al. does not expressly disclose compressing the received audio device identification information; and generating a hash value of the compressed audio device identification information to form a requested device authentication initialization token. However, Examiner takes Official Notice that the use of compression of identification information and generating hash values of identification information was well known in the art at the time the invention was made. Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to compress the received audio device identification information; and to generate a hash value of the compressed audio device identification information to form the authentication initialization token of the wireless device since Examiner takes Official Notice that it was conventional and well known.

Regarding claims 8 and 18, the combination of Nakakita et al., Cook et al., and Rowland et al. teach the limitations as set forth under claims 1 and 11 respectively above. Furthermore, Cook et al. teach receiving an audio authentication token as the requested audio authentication/ identification information of the detected wireless device (column 7, lines 15-67, column 8, lines 1-67); comparing the received audio authentication token to one or more stored audio authentication tokens (column 7, lines

50-67); when a matching stored audio authentication token is detected, establishing an audio link with the detected wireless device (column 7, lines 50-67, column 8, lines 1-50); and storing the requested device identification information as a device authentication token of the detected wireless devices (column 7, lines 50-67, column 8, lines 1-50).

Regarding claims 9 and 19, the combination of Nakakita et al., Cook et al., and Rowland et al. teach the limitations as set forth under claims 8 and 18 respectively above. Furthermore, Rowland et al. teach otherwise, requesting manual authorization from a user of the host device to authenticate the detected wireless device (switching to different authentication methods, page 5, paragraph 76-78). Nakakita et al. teach when the user provides manual authentication authorization, storing the requested device identification information (as a device authentication token) of the detected wireless device (column 10, lines 1-67). Cook et al. teach establishing an audio link between the detected wireless device and the host device (column 7, lines 50-67, column 8, lines 1-50).

Regarding claims 10 and 20, the combination of Nakakita et al., Cook et al., and Rowland et al. teach the limitations as set forth under claims 1 and 11 respectively above. Furthermore, Nakakita et al. teach requesting the device identification information from the detected wireless device (column 7, lines 45-67, column 8, lines 1-67, column 9, lines 1-67); and receiving one of an authentication device key and a device identification code and a device personal identification number from the detected wireless device as the requested identification information (column 10, lines 45-67).

8. Claims 21, 25-26, 28, 30-33 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakakita et al., and further in view of Cook et al.

Regarding claim 21, Nakakita et al. teach receiving, by a wireless device, a communications connection request from a host device (column 9-10); when a request for authentication initialization information is received from the host device, providing authentication initialization information to the host device (column 10); and once the audio authentication initialization information is authenticated by the host device, establishing an link between the wireless device and the host device (column 10, lines 30-45). Nakakita et al. do not disclose expressly using audio authentication information. However, Cook et al. teach the use of wireless voice authentication and transaction validation, a microphone to receive a speech sample from the device user, and transferring the speech sample from the wireless device to the wireless interface (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on received audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 25, the combination of Nakakita et al. and Cook et al. teaches the limitations as set forth under claim 26 above. Furthermore, Cook et al. teach receiving a device authentication set-up request from a user of the wireless device (column 7, lines 50-67); requesting, from the user, audio device identification information as audio authentication initialization information of the wireless device

(column 7, lines 50-67); and once the audio device identification information is received from the user, storing the voice audio device identification information as an audio authentication initialization token of the wireless device (column 7, lines 50-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 26, Nakakita et al. teach receiving, by a wireless device, a connection request from a host device (column 9-10); when a request for authentication initialization information is received from the host device, providing authentication initialization information to the host device (column 10); and once the authentication initialization information is authenticated by the host device, establishing a link between the wireless device and the host device (column 10, lines 30-45). Nakakita et al. do not disclose expressly using audio authentication information. However, Cook et al. teach the use of wireless voice authentication and transaction validation, a microphone to receive a speech sample from the device user, and transferring the speech sample from the wireless device to the wireless interface (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on received audio authentication from the device. One of ordinary skill in the art would have been

motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 28, the combination of Nakakita et al. and Cook et al. teaches the limitations as set forth under claim 26 above. Furthermore, Cook et al. teach requesting audio authentication initialization information from a user of the wireless device; receiving audio device identification information from the user as the authentication initialization information of the detected wireless device; and providing the audio device identification information to the host device as the requested audio authentication initialization information (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 30, the combination of Nakakita et al. and Cook et al. teaches the limitations as set forth under claim 26 above. Furthermore, Cook et al. teach receiving a device initialization request from a user of the wireless device (column 7, lines 50-67); requesting, from the user, audio device identification information as audio authentication initialization identification information of the wireless device (column 7, lines 50-67); and once the audio device identification information of the wireless device is received, storing the audio device identification information as an authentication initialization token of the wireless device (column 7, lines 50-67). Therefore, it would

have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 31, Nakakita et al. teach an authentication unit to authenticate wireless devices detected within communications range of the apparatus using authentication initialization information of the detected wireless device (column 9-10); a communications interface coupled to the authentication unit, the communications interface to establish links with authenticated wireless devices, request device identification information as well as device authentication initialization information from detected wireless devices (column 10); and a storage device coupled to the authentication unit, containing an authentication initialization token as well as an authentication key for each wireless device initialized by the apparatus (column 9, lines 40-67). Nakakita et al. do not disclose expressly authenticating the device by using audio authentication information. However, Cook et al. teach the use of wireless voice authentication and transaction validation, a microphone to receive a speech sample from the device user, and transferring the speech sample from the wireless device to the wireless interface (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 32, the combination of Nakakita et al. and Cook et al. teaches the limitations as set forth under claim 31 above. Furthermore, Nakakita et al. teach a device initialization unit to request audio device identification information in response to a device authentication set-up request from a user of a wireless device and store the received device identification information as an authentication initialization token of the wireless device (column 9, lines 10-67, column 10, lines 1-61). Nakakita et al. do not disclose expressly using audio authentication. However, Cook et al. teach the use of wireless voice authentication and transaction validation, a microphone to receive a speech sample from the device user, and transferring the speech sample from the wireless device to the wireless interface (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 33, the combination of Nakakita et al. and Cook et al. teaches the limitations as set forth under claim 31 above. Furthermore, Nakakita et al. teach wherein the authentication unit compares a received authentication initialization token to one or more stored authentication initialization tokens, establishes a link with a detected wireless device when a matching stored authentication initialization token is detected, and stores requested device identification information of the detected wireless device as an authentication key (column 10, lines 30-45). Nakakita et al. do not disclose expressly

using audio authentication. However, Cook et al. teach the use of wireless voice authentication and transaction validation, a microphone to receive a speech sample from the device user, and transferring the speech sample from the wireless device to the wireless interface (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

9. Claims 22-24, 27, 29 are rejected under 35 U.S.C. 103(a) as being unpatentable over Nakakita et al. and Cook et al., and further in view of Rowland et al.

Regarding claim 22, Nakakita et al. teach receiving a request for device identification information of the wireless device (column 10, lines 15-30); providing the requested device identification information to the host device (column 10, lines 15-30). The combination of Nakakita et al. and Cook et al. do not expressly teach when the requested device identification information of the wireless device is not authenticated by the host device, receiving a request for audio authentication initialization information of the detected wireless device. However, Rowland et al. teach switching to different authentication methods (page 5, paragraph 76-78). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to switch authentication methods after a first authentication method used does not authenticate a device. One of ordinary skill in the art would have been motivated to do

so to provide an alternative authentication method on the event of a security compromise (Rowland et al., page 5, paragraph 76).

Regarding claim 23, the combination of Nakakita et al., Cook et al., and Rowland et al. teaches the limitations as set forth under claim 22 above. Furthermore, Cook et al. teach requesting audio authentication initialization information from a user of the wireless device; receiving audio device identification information from the user as the authentication initialization information; and providing the audio device identification information to the host device as the requested audio authentication initialization information (column 7, lines 15-67, column 8, lines 1-67). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio authentication from the device. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 24, the combination of Nakakita et al., Cook et al., and Rowland et al. teaches the limitations as set forth under claim 22 above. Furthermore, Cook et al. teach the use of voice authentication and transaction validation (column 7, lines 15-67, column 8, lines 1-67) and Rowland et al. teach switching to different authentication methods (page 5, paragraph 76-78). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to select a stored audio authentication initialization token; and to transmit the audio authentication initialization token to the host device. One of ordinary skill in the art would have been

motivated to do so because it was well known in the art to provide authentication token to a host device.

Regarding claim 27, Nakakita et al. teach receiving a request for device identification information of the wireless device (column 10, lines 15-30); providing the requested device identification to the host device (column 10, lines 15-30). The combination of Nakakita et al. and Cook et al. do not expressly teach when the requested authentication information of the wireless device; is not authenticated by the host device, receiving a request for audio authentication initialization information of the detected wireless device. However, Rowland et al. teach switching to different authentication methods (page 5, paragraph 76-78). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to switch authentication methods after a first authentication method used does not authenticate a device. One of ordinary skill in the art would have been motivated to do so to provide an alternative authentication method on the event of a security compromise (Rowland et al., page 5, paragraph 76).

Regarding claim 29, the combination of Nakakita et al., Cook et al., and Rowland et al. teaches the limitations as set forth under claim 27 above. Furthermore, Cook et al. teach the use of voice authentication and transaction validation (column 7, lines 15-67, column 8, lines 1-67) and Rowland et al. teach switching to different authentication methods (page 5, paragraph 76-78). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to select a stored audio authentication initialization token; and to transmit the audio authentication

initialization token to the host device. One of ordinary skill in the art would have been motivated to do so because it was well known in the art to provide authentication token to a host device.

10. Claims 34-36 are rejected under 35 U.S.C. 103(a) as being unpatentable over Cook et al., and further in view of Lemiläinen et al. (US Patent Number: 6,766,160).

Regarding claim 34, Cook et al. teach a system comprising: a host device (column 3, lines 17-67, the base station); and one or more wireless devices, each wireless device including: a processor having circuitry to execute instruction; and a storage device having a sequence of instructions stored therein (column 3, lines 17-67). Cook et al. also teach the use of wireless voice authentication and transaction validation, a microphone to receive a speech sample from the device user, and transferring the speech sample from the wireless device to the wireless interface (column 7, lines 15-67, column 8, lines 1-67). Cook et al. do not disclose expressly authenticating the device by using voice authentication information. However, Lemiläinen et al. teach authenticating a mobile terminal (column 6, lines 25-62). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio device identification from the user. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 35, the combination of Cook et al. and Lemiläinen et al. teaches the limitations as set forth under claim 34 above. Furthermore, Cook et al. teach an authentication unit to authenticate wireless devices detected within communications range of the host device using audio authentication information of the detected wireless devices (column 7, lines 15-67, column 8, lines 1-67); a communications interface coupled to the authentication unit, the communications interface to establish audio links with authenticated wireless devices, request device identification information as well as audio authentication initialization information from detected wireless devices (column 7, lines 15-67, column 8, lines 1-67). Cook et al. do not disclose expressly a storage device coupled to the authenticating unit, containing an audio authentication initialization tokens as well as device identification information for each wireless device initialized by the host device. However, Lemiläinen et al. teach a storage device coupled to the authenticating unit, containing an audio authentication initialization tokens as well as device identification information for each wireless device initialized by the host device (column 6, lines 25-52). Therefore, it would have been obvious to one having ordinary skill in the art at the time the invention was made to authenticate a device based on receiving audio device identification from the user. One of ordinary skill in the art would have been motivated to do so because at the time the invention was made the use of voice/audio authentication was well known in the art.

Regarding claim 36, the combination of Cook et al. and Lemiläinen et al. teaches the limitations as set forth under claim 34 above. Furthermore, Lemiläinen et al. teach a device initialization unit to request an audio device identification in response to a device

authentication set-up request from a user of a wireless device and store received audio device identification information as an authentication initialization token for the wireless device (column 6, lines 25-52). The motivation for the combination is the same as stated above, for claim 34.

Conclusion

11. Any inquiry concerning this communication or earlier communications from the examiner should be directed to David G. Cervetti whose telephone number is (571) 272-5861. The examiner can normally be reached on Monday-Friday 7:00 am - 5:00 pm, off on Wednesday.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz R. Sheikh can be reached on (571) 272-3795. The fax phone number for the organization where this application or proceeding is assigned is 703-872-9306.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free).

DGC

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100